THE PUBLISHING HOUSE
OF THE ROMANIAN ACADEMY

PROCEEDINGS OF THE ROMANIAN ACADEMY, Series A,
Volume 16, Special Issue 2015, pp. 265-270

INTEGRAL CRYPTANALYSIS OF ROUND-REDUCED PRINCE CIPHER

Raluca POSTEUCA[1], Gabriel NEGARA[2]

[1]University of Bucharest, Romania
[2]Al. I. Cuza University of Iaşi, Romania
E-mail: raluca.e.posteuca@gmail.com

The lightweight cryptographic algorithm Prince is an intensively studied cipher in the last 3 years. In order to enhance the cryptanalysis efforts and to encourage the design of practical attacks against the algorithm, the designers organized the Prince Challenge. In this paper we introduce two integral attacks on 5-round and 6-round reduced Prince. The attacks, based on a 4.5 rounds integral distinguisher, lead to the full key recovery and have practical complexity. The 6-round attack was submitted to the second round of The Prince Challenge and was announced as winner during the Rump Session of the Eurocrypt 2015 Conference.

Key words: Prince Cipher, lightweight cryptography, Prince Challenge, integral cryptanalysis, integral distinguisher, practical complexity.

1. INTRODUCTION

1.1. The Prince Cipher

The area of lightweight cryptography involves ciphers with low implementation costs, adequate for use in smart devices that have very limited resources (regarding memory, computing power, battery supply). More and more applications will process sensitive personal data, such as medical and biometric data, so the demand for lightweight cryptographic primitives is continuously increasing. The design of each such primitive must deal with trade-offs between security, cost, and performance [1].

The Prince Cipher description was first published in [2], the paper being published at ASIACRYPT 2012. The cipher's design was optimized in order to fulfill hardware implementation restrictions and real-time security needs, commonly met in the field of lightweight cryptography.

Prince is a block cipher that processes 64-bit blocks, using a 128-bit key and 12 layers of S-boxes. The key schedule is simplified compared to classical block ciphers; the operation involved performing an expansion of the 128-bit key to a 196-bit key.

The enciphering process involves an initial whitening operation, five rounds (named forward rounds for the rest of the paper), a middle linear layer (named middle rounds), followed by other five rounds (which use the inverse of the forward rounds operations, so we will call them backward rounds) and a final whitening operation. Each round consists of an S-box layer, an M-Layer (composed by a Shift Rows operation, similar to the one used in AES, and a multiplication layer) and a constant XOR addition, followed by a key XOR operation (the same 64-bit key is used for each of the 12 rounds of the cipher).

Regarding implementation performance, an important characteristic is that the cipher holds the so called α-property: the deciphering function is identical to the enciphering function, when using a slightly different key mathematically related to the enciphering key. Due to this property, the implementation of the deciphering function do not involve additional resources compared to the enciphering function implementation.

1.2. The Prince Challenge

In order to encourage the cipher's cryptanalysis and to increase the knowledge about the algorithm's cryptographic resistance against practical attacks, Technical University of Denmark (DTU), NXP Semiconductors and the Ruhr University Bochum proposed The Prince Challenge [3]. Specialists from both academia and industry are invited to contribute to this competition.

The first round of this competition ended before Crypto 2014 Conference, while the second one ended before Eurocrypt 2015 Conference. The third round is in progress, the submission deadline being April 2016. All the rounds involve 2 settings, one in the chosen-plaintext attack scenario, and the other in the known-plaintext attack scenario.

Due to the fact that the competition aims at finding practical attacks, the submissions must respect some initial restrictions regarding the data, time and memory complexity.

This paper mainly presents the integral attack that was designated as the winner of the second round of the Prince Challenge, in the 6-round reduced Prince scenario.

1.3. Related work

The Prince cipher's cryptanalysis work includes mainly theoretical attacks round-reduced and full Prince and also a number of practical attacks on round-reduced versions of the algorithm.

Derbez and Perrin describe in [4] a few attacks based on a meet-in-the-middle approach, applicable (theoretically) up to 10 rounds of the algorithm. These attacks won the sections for 6-round and 8-round reduced Prince in the first round of the Prince Challenge (in the chosen-plaintext scenario); in the same round Derbez also won the 4-round and 6-round sections in the known-plaintext setting. In [4] they also described how can be used a modified SAT solver in order to design a practical attack on 4 rounds of Prince and it is introduced a 6-round differential attack.

In [5] Morawiecki introduces attacks relying on integral and higher-order differential cryptanalysis, up to 7 rounds. One of the attacks won the section dedicated to 4 round-reduced Prince in the first round of the competition (chosen-plaintext attack).

Various other results on Prince involve attacks based on truncated and multiple differentials, meet-in-the-middle approaches, reflection cryptanalysis, biclique and differential cryptanalysis [3], etc.

2. INTEGRAL CRYPTANALYSIS

2.1. General description

Integral cryptanalysis represents a class of attacks particularly applicable to block ciphers based on substitution-permutation networks. The approach was introduced by Lars Knudsen as a dedicated attack against the Square cipher [6], and then extended to other ciphers related to Square.

Integral cryptanalysis uses sets of chosen plaintexts for which a part of the data is constant and the remaining part varies through all possibilities. The corresponding ciphertexts, after a partial decryption, are used in order to recover parts of the secret key (by checking for some properties of the intermediate ciphertexts obtained after this type of decryption, usually a XOR sum equal to zero).

A recent result in the integral cryptanalysis of Prince is the one described by Morawiecki in [5]. The paper presents a 3.5 round distinguisher on Prince. The design of the distinguisher starts with one active nibble and after 3.5 rounds the XOR sum of all nibbles is 0 (i.e. the nibbles are still balanced). As proved in the paper, a subsequent S-box layer destroys this property. Using the distinguisher, Morawiecki implemented a 4-round attack on Prince, which he was able to extend to 6 rounds, adding an initial and a final round.

2.2. Our distinguisher on 4.5-round Prince

Starting from [5], we found a 4.5-round integral distinguisher for Prince.

In our designs, one block of data is represented as an array containing 16 nibbles, indexed as follows: {0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15}.

The distinguisher starts from three active nibbles and after 4.5 rounds, all nibbles are balanced. We start with a set of 2^{12} plaintexts (obtained by iterating all the possible values of the 3 active nibbles, and keeping constant the remaining 13 nibbles) and we encipher it with 4.5 rounds of Prince (two forward rounds, the middle rounds and one incomplete backward round – without the S-Layer). Our distinguisher is based on the property that the XOR sum of the 2^{12} ciphertexts is equal to 0 (all 16 nibbles of the XOR sum are equal to 0).

The position of the three active nibbles is not arbitrary, they must be placed on a set of *4* consecutive nibbles of the type $\{4i, 4i+1, 4i+2, 4i+3\}$, with i ranging from 0 to 3. There are 16 possible combinations of positions for the 3 active nibbles, for which the distinguisher holds. In our implementations we chose as active the first three nibbles.

The property will not hold if an additional S-box layer is applied. Using this distinguisher, we implemented a 5-round attack on Prince (similar to Morawiecki's 4-round attack), and then we extended this attack to 6-rounds, by adding one final round.

Observation: In the description of our attacks, we denoted the final whitening key by k_0 (instead of k'_0).

2.3. The 5-round integral attack on Prince

For the implementation of this attack, we encrypt a set of 2^{12} plaintexts (obtained by iterating all the possible values of the first three nibbles) with 5 rounds of Prince (two forward rounds, the middle layer and one backward round). For each value of one nibble from $k_0 \oplus k_1$, we partially decrypt the set of 2^{12} ciphertexts through the last S-box and check whether the XOR sum of all the resulting nibbles is 0. If the sum is 0, then the guessed nibble is probably the right one. We will repeat these steps for all 16 nibbles from $k_0 \oplus k_1$. Thus, data complexity is $2 \cdot 2^{12}$ chosen plaintexts. Time complexity is equal to $2 \cdot 2^{12}$ (plaintexts) $\cdot$ 2^4 (one nibble exhaustive search) $\cdot$ 2^4 (number of nibbles) = 2^{21}.

The pseudocode of the 5-*round integral attack*:

1. *Generate* a set of 2^{12} plaintexts in which the first three nibbles (indexes 0, 1, 2) are active (iterate all possible values)
2. *Encrypt* each plaintext from the set using *5-round* Prince cipher, obtaining the set of 2^{12} corresponding ciphertexts
3. *Foreach* nibble position *POS* (from 0 to 15) of the key $k_0 \oplus k_1$
   Foreach possible value k_v (from 0 to 15) of the *POS* nibble from $k_0 \oplus k_1$
   i. *Partially decrypt* (obtaining only the nibble with the index *POS*) of each of the ciphertexts, by applying the *S-layer*
   ii. *Compute* the *XOR* sum of the 2^{12} obtained nibble values
   iii. *If* the *XOR* sum is 0
   - keep k_v as probable value of the nibble from position *POS* of the key $k_0 \oplus k_1$

   End if
   End foreach
   End foreach

Observation: After only one application of the attack, some false positives can be obtained; in order to filter them, we run the attack for 2 sets of plaintexts (2 sets were sufficient to eliminate all false positives); In this way, all 64 bits of $k_0 \oplus k_1$ will be obtained.

2.4. The 6-round integral attack on Prince

We extended the 5-round attack to 6 rounds by adding one final round. The attack operates by guessing at once a set of 4 nibbles of $k_0 \oplus k_1$ and 1 nibble of k_1, instead of only *1* nibble, in the case of the 5-round attack. More precisely, we are able to partially decrypt sets of 4 nibbles of the ciphertexts through the *S-layer* and *M-layer*. Then, we guess one nibble of k_1 and partially decrypt, through the *S-layer*, 1 nibble of the set of 2^{12} intermediate texts (obtained after the first partial decryption). If the guesses are correct, the *XOR* sum of the 2^{12} values of the targeted nibble should be 0 (according to our 4.5-round distinguisher).

For the 12 remaining nibbles of k_1, we will fully decrypt (through one round) the set of 2^{12} ciphertexts, using the fact that we recovered at this point all the values of $k_0 \oplus k_1$, and then we will apply the 5-round attack previously described.

Thus, data complexity is of $6 \cdot 2^{12}$ chosen plaintexts. Time complexity is equal to $6 \cdot 2^{12}$ (plaintexts) $\cdot$ 2^2 (sets of 4 nibbles) $\cdot$ $2^{4(4+1)}$ (exhaustive search on 4 + 1 nibbles) + $6 \cdot 2^{12}$ (plaintexts) $\cdot$ 2^4 (one nibble exhaustive search) $\cdot$ 12 (number of nibbles) $\simeq 2^{37}$.

The pseudocode for the 6-*round integral attack*:

1. *Generate* a set of 2^{12} plaintexts in which the first three nibbles (indexes 0, 1, 2) are active (take all possible values)
2. *Encrypt* each plaintext from the set using 6-*round* Prince cipher, obtaining the set of 2^{12} corresponding ciphertexts;
3. *For i* from 0 to 3
   Foreach possible values V_i of nibbles $\{4i, 4i+1, 4i+2, 4i+3\}$ from $k_0 \oplus k_1$
   i. *Partially decrypt* each ciphertext, by applying the *S-layer* and the *M-Layer* obtaining only the nibbles $\{4i, 4i+1, 4i+2, 4i+3\}$
   ii. *Foreach* possible value k_v of the nibble $4i$ from k_1,
   a) *Partially decrypt*, through the *S-layer*, the nibble $4i$ obtained in step *i*.
   b) *Compute* the *XOR* sum of the 2^{12} obtained values
   c) *If* the *XOR* sum is 0
   - *keep* V_i as probable values of nibbles $\{4i, 4i+1, 4i+2, 4i+3\}$ from $k_0 \oplus k_1$
   - *keep* k_v as probable value of nibble $4i$ from the key k_1

   End if
   End foreach
   End foreach
   End for

   At this point, we recovered the full $k_0 \oplus k_1$ and 4 nibbles from k_1 (indexes 0, 4, 8 and 12)
4. *Fully decrypt* the last round of each ciphertext (using the full key $k_0 \oplus k_1$)
5. *Foreach* nibble position *POS* from {1, 2, 3, 5, 6, 7, 9, 10, 11, 13, 14, 15} of the key k_1
   Foreach possible value k_v (from 0 to 15) of the *POS* nibble from k_1
   Foreach ciphertext *C* obtained in step 4.
   i. *Partially decrypt* (obtaining only the nibble with the index *POS*) of each of the ciphertext *C*, by applying the *S-layer*
   ii. *Compute* the *XOR* sum of the 2^{12} obtained values
   iii. *If* the *XOR* sum is 0
   - *keep* k_v as probable value of nibble *POS* in the key k_1

   End if
   End foreach
   End foreach
   End foreach

Observation: Some false positives can be obtained when running the attack; in order to filter them, we used 6 sets of plaintexts (6 sets were sufficient to eliminate all false positives); we are able to recover the full $k_0 \oplus k_1$ and the full k_1, so the full k_0 can be computed.

2.5. Comparison with other 6-round attacks

Compared with the attack of Derbez and Perrin [4], in which they obtained 33 key bits, we were able to recover all 128 key bits.

The data and time complexity of the existing attacks on 6-*round* PRINCE that we studied are synthesized in Table 1.

Table 1

Comparison between 6-round attacks on Prince

Authors	**Attack Type**	**Time Complexity**	**Data Complexity**	**Stored Data**
Derbez and Perrin [4]	Meet-in-the-middle	$2^{33.7}$	2^{16}	$2^{31.9}$
Morawiecki [5]	Integral	2^{41}	$6 \cdot 2^{16}$	-
Our attack	Integral	2^{37}	$6 \cdot 2^{12}$	-

By comparing with the results of Derbez and Perrin, the data complexity of our attack is reduced by a factor of approximately $2^{1.4}$, while compared with Morawiecki's attack, the improvement has a factor of 2^4. As far as we know, there are no currently known attacks for 6-round Prince that have data complexity smaller than our attack ($6 \cdot 2^{12}$). One can observe that we improved Morawiecki's attack (we obtained a time complexity smaller than 2^{41}). On the other hand, compared with Derbez and Perrin results, our attack has higher time complexity (2^{37} instead of $2^{33.7}$), but no data storage is required (Derbez and Perrin attack needs $2^{31.9}$ bytes of memory).

3. CONCLUSION. FUTURE WORK

In this paper we introduce new practical integral attacks on 5-round and 6-round reduced Prince cipher. Future work will aim at extending the attack to more rounds while trying to maintain low data, time and memory complexity. Also, we intend to design and apply other types of cryptanalytic techniques against reduced or full Prince cipher.

Regarding the implementation of our attacks, we wrote at this point only sequential C# programs, using Microsoft Visual Studio 2013 and .NET Framework 4.5. Due to their design, the attacks can be implemented using parallel approaches (subsets of plaintexts can be enciphered in parallel, and also the exhaustive search process of different key nibbles values can be split using parallelization).

REFERENCES

1. T. EISENBARTH, S. KUMAR, C. PAAR, A. POSCHMANN, L. UHSADEL, *PRINCE A Survey of Lightweight Cryptography Implementations*, IEEE Design & Test of Computers, 2007.
2. J. BORGHOFF, A. CANTEAUT, *PRINCE – A Low-Latency Block Cipher for Pervasive Computing Applications*, Springer, Advances in Cryptology, pp. 208-225, ASIACRYPT, 2012.
3. *The Prince Challenge*, Technical University of Denmark (DTU), NXP Semiconductors and the Ruhr University Bochum, https://www.emsec.rub.de/research/research_startseite/prince-challenge, 2015.
4. P. DERBEZ, L. PERRIN, *Meet-in-the-Middle Attacks and Structural Analysis of Round-Reduced PRINCE*, FSE 2015, eprint 2015/239.
5. P. MORAWIECKI, *Practical Attacks on the Round-reduced PRINCE*, eprint 2015/245.
6. J. DAEMEN, L.R. KNUDSEN, V. RIJMEN, T*he block cipher square*, FSE, pp. 149–165, 1997.